DPA & GDPR
Standard Contractual Clauses for PII processing
and data transfers between EU and Non-EU Countries

Standard Contractual Clauses

Between:

bluesource Information Limited
and
Fuse Technology Pty Ltd.

According to the General Data Protection Regulation (GDPR), contractual clauses ensuring appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries. This includes model contract clauses – so-called standard contractual clauses (SCCs) – that have been "pre-approved" by the European Commission.

On 4 June 2021, the Commission issued modernised standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR):

These modernised SCCs replace the three sets of SCCs that were adopted under the previous Data Protection Directive 95/46 and since 27 September 2021, it is no longer possible to conclude contracts incorporating these earlier sets of SCCs.

For this reason, any Model Clauses agreed between the parties detailed in Annex I.A, each a "P**arty**" and together "**the Parties"**, prior to the 27 September 2021 are not valid for new contracts after this date and the Parties agree to enter in to these replacement "Standard Contruactual Clauses" in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in Annex I.B.

EUROPEAN
COMMISSION

Brussels, 4.6.2021
C(2021) 3972 final

ANNEX

ANNEX

to the

COMMISSION IMPLEMENTING DECISION

**on standard contractual clauses for the transfer of personal data to third countries
pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council**

ANNEX

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a)   The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b)   The Parties:

   (i)   the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "**Data Exporter**"), and

   (ii)   the entity/ies in a third country receiving the personal data from the Data Exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "**Data Importer**")

   have agreed to these standard contractual clauses (hereinafter: "**Clauses**").

(c)   These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d)   The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a)   These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid

---

[1]   Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b)   These Clauses are without prejudice to obligations to which the Data Exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a)   Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the Data Exporter and/or Data Importer, with the following exceptions:

   (i)   Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

   (ii)   Clause 8 - Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);

   (iii)   Clause 9 - Clause 9(a), (c), (d) and (e);

   (iv)   Clause 12 - Clause 12(a), (d) and (f);

   (v)   Clause 13;

   (vi)   Clause 15.1(c), (d) and (e);

   (vii)   Clause 16(e);

   (viii) Clause 18 - Clause 18(a) and (b);

(b)   Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a)   Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b)   These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c)   These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

<div align="center">

Clause 7 - Optional

Docking clause

</div>

(a)   An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a Data Exporter or as a Data Importer, by completing the Appendix and signing Annex I.A.

(b)   Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a Data Exporter or Data Importer in accordance with its designation in Annex I.A.

(c)   The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

<div align="center">

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

</div>

The Data Exporter warrants that it has used reasonable efforts to determine that the Data Importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

For the purposes of these Standard Contractual Clauses:

- Whilst the Data Exporter is a controller for its Support Data (contracts, support tickets, documentation, invoices, purchase orders, statements of work, etc.), it is contracturaly classified as a processor in customer contracts in relation to customer data.

- the Date Importer is a "Data Processor" on behalf of the Data Exporter.

8.1   Instructions

(a)   The Data Exporter has informed the Data Importer that it acts as processor under the instructions of its controller(s), which the Data Exporter shall make available to the Data Importer prior to processing.

(b)   The Data Importer shall process the personal data only on documented instructions from the controller, as communicated to the Data Importer by the Data Exporter, and any additional documented instructions from the Data Exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or Data Exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c)   The Data Importer shall immediately inform the Data Exporter if it is unable to follow those instructions. Where the Data Importer is unable to follow the instructions from the controller, the Data Exporter shall immediately notify the controller.

(d)   The Data Exporter warrants that it has imposed the same data protection obligations on the Data Importer as set out in the contract or other legal act under Union or Member State law between the controller and the Data Exporter[2].

---

[2] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

8.2 Purpose limitation

The Data Importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the Data Importer by the Data Exporter, or from the Data Exporter.

8.3 Transparency

On request, the Data Exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Data Exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the Data Importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the Data Exporter without undue delay. In this case, the Data Importer shall cooperate with the Data Exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the Data Importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the Data Importer shall, at the choice of the Data Exporter, delete all personal data processed on behalf of the controller and certify to the Data Exporter that it has done so, or return to the Data Exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the Data Importer that prohibit return or deletion of the personal data, the Data Importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the Data Importer under Clause 14(e) to notify the Data Exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a)   The Data Importer and, during transmission, also the Data Exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where

possible, remain under the exclusive control of the Data Exporter or the controller. In complying with its obligations under this paragraph, the Data Importer shall at least implement the technical and organisational measures specified in Annex II. The Data Importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b)   The Data Importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c)   In the event of a personal data breach concerning personal data processed by the Data Importer under these Clauses, the Data Importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The Data Importer shall also notify, without undue delay, the Data Exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d)   The Data Importer shall cooperate with and assist the Data Exporter to enable the Data Exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the Data Importer.

8.7   Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the Data Importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8   Onward transfers

The Data Importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the Data Importer by the Data Exporter. In addition, the data may only be disclosed to a third party located outside the European Union[3] (in the same country as the Data Importer or in another third country, hereinafter

---

[3]   The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

"onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the Data Importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The Data Importer shall promptly and adequately deal with enquiries from the Data Exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the Data Importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The Data Importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the Data Exporter, which shall provide it to the controller.

(d) The Data Importer shall allow for and contribute to audits by the Data Exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the Data Exporter requests an audit on instructions of the controller. In deciding on an audit, the Data Exporter may take into account relevant certifications held by the Data Importer.

(e) Where the audit is carried out on the instructions of the controller, the Data Exporter shall make the results available to the controller.

(f) The Data Exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the Data Importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a)   SPECIFIC PRIOR AUTHORISATION The Data Importer shall not sub-contract any of its processing activities performed on behalf of the Data Exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The Data Importer shall submit the request for specific authorisation at least 30 days prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the Data Exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

(b)   Where the Data Importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the Data Importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[4] The Parties agree that, by complying with this Clause, the Data Importer fulfils its obligations under Clause 8.8. The Data Importer shall ensure that the sub-processor complies with the obligations to which the Data Importer is subject pursuant to these Clauses.

(c)   The Data Importer shall provide, at the Data Exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the Data Importer may redact the text of the agreement prior to sharing a copy.

(d)   The Data Importer shall remain fully responsible to the Data Exporter for the performance of the sub-processor's obligations under its contract with the Data Importer. The Data Importer shall notify the Data Exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e)   The Data Importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the Data Importer has factually disappeared, ceased to exist in law or has become insolvent - the Data Exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a)   The Data Importer shall promptly notify the Data Exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b)   The Data Importer shall assist, where appropriate in cooperation with the Data Exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or

---

[4]   This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c)   In fulfilling its obligations under paragraphs (a) and (b), the Data Importer shall comply with the instructions from the controller, as communicated by the Data Exporter.

Clause 11

Redress

(a)   The Data Importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b)   In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c)   Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the Data Importer shall accept the decision of the data subject to:

    (i)   lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

    (ii)   refer the dispute to the competent courts within the meaning of Clause 18.

(d)   The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e)   The Data Importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f)   The Data Importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a)   Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b)   The Data Importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the Data Importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c)   Notwithstanding paragraph (b), the Data Exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the Data Exporter or the Data Importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the Data Exporter and, where the Data Exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d)   The Parties agree that if the Data Exporter is held liable under paragraph (c) for damages caused by the Data Importer (or its sub-processor), it shall be entitled to claim back from the Data Importer that part of the compensation corresponding to the Data Importer's responsibility for the damage.

(e)   Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f)   The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g)   The Data Importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a)   As the Data Exporter is based in the United Kindom, which is no longer an EU Member State, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

     The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b)   The Data Importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the Data Importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a)   The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the Data Importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the Data Importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b)   The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

   (i)   the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

   (ii)   the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[5];

   (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c)   The Data Importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the Data Exporter with relevant information and agrees that it will continue to cooperate with the Data Exporter in ensuring compliance with these Clauses.

(d)   The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e)   The Data Importer agrees to notify the Data Exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in

---

[5]   As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

practice that is not in line with the requirements in paragraph (a). The Data Exporter shall forward the notification to the controller.

(f)   Following a notification pursuant to paragraph (e), or if the Data Exporter otherwise has reason to believe that the Data Importer can no longer fulfil its obligations under these Clauses, the Data Exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the Data Exporter and/or Data Importer to address the situation, if appropriate in consultation with the controller. The Data Exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the Data Exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the Data Exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the Data Importer in case of access by public authorities

15.1   Notification

(a)   The Data Importer agrees to notify the Data Exporter and, where possible, the data subject promptly (if necessary with the help of the Data Exporter) if it:

(i)   receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii)   becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The Data Exporter shall forward the notification to the controller.

(b)   If the Data Importer is prohibited from notifying the Data Exporter and/or the data subject under the laws of the country of destination, the Data Importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The Data Importer agrees to document its best efforts in order to be able to demonstrate them on request of the Data Exporter.

(c)   Where permissible under the laws of the country of destination, the Data Importer agrees to provide the Data Exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The Data Exporter shall forward the information to the controller.

(d)   The Data Importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e)   Paragraphs (a) to (c) are without prejudice to the obligation of the Data Importer pursuant to Clause 14(e) and Clause 16 to inform the Data Exporter promptly where it is unable to comply with these Clauses.

15.2   Review of legality and data minimisation

(a)   The Data Importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The Data Importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the Data Importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the Data Importer under Clause 14(e).

(b)   The Data Importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter. It shall also make it available to the competent supervisory authority on request. The Data Exporter shall make the assessment available to the controller.

(c)   The Data Importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a)   The Data Importer shall promptly inform the Data Exporter if it is unable to comply with these Clauses, for whatever reason.

(b)   In the event that the Data Importer is in breach of these Clauses or unable to comply with these Clauses, the Data Exporter shall suspend the transfer of personal data to the Data Importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c)   The Data Exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i)   the Data Exporter has suspended the transfer of personal data to the Data Importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii)   the Data Importer is in substantial or persistent breach of these Clauses; or

(iii)   the Data Importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the Data Exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d)   Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the Data Exporter immediately be returned to the Data Exporter or deleted in its entirety. The same shall apply to any copies of the data. The Data Importer shall certify the deletion of the data to the Data Exporter. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred personal data, the Data Importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e)   Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of England and Wales.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of England and Wales.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as Data Exporter(s) and/or Data Importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data Exporter(s):

Name: Bluesource Information Limited

Address: 122 Tooley Street, London, SE1 2TU United Kingdom

Contact person's name, position and contact details:

        Nick Jaggers, Head of Operations, nick.jaggers@bluesource.co.uk,

        +44(0)2079406220

Activities relevant to the data transferred under these Clauses:

        Processing Support Data, Data Exporter's and their customer's personal data as reasonably necessary to maintain the relationship and provide contracted services to the Data Exporter and the Data Exporter's customers.

        "Support Data" all data, including all text, sound, video, image files, or software, that are provided to Data Exporter by or on behalf of the Data Exporter's customer or produced during the relationship between the parties, such as and not limited to support tickets, project documentation, contracts, purchase orders, invoices, and emails.

Signature and date: [*Jaggers* 7F389F108A56489...] on [17/1/2024].

Role (controller/processor): Processor of customer owned data and controller of Support Data

Data Importer(s): [*Identity and contact details of the Data Importer(s), including any contact person with responsibility for data protection*]

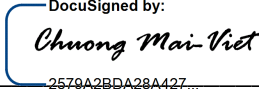1. Name: Fuse Technology (PTY) Ltd   (in Australia)

Address: Suite 2, Level 9, 420 George Street, Sydney NSW 2000, Australia

Contact person's name, position and contact details:

> Chuong Mai-Viet, Managing Director, chuong@fusetechnology.com.au

Activities relevant to the data transferred under these Clauses:

> Processing Support Data, Data Exporter's and their customer's personal data as reasonably necessary to maintain the relationship and provide contracted services to the Data Exporter and the Data Exporter's customers.

Signature and date: [*Chuong Mai-Viet* 2579A2BDA28A427…] on [17/1/2024].

Role (controller/processor):   Processor

2. Name: Fuse Technology (PTY) Ltd (in Vietnam)

Address: 23floor, Wework, Etown Central - 11 Doan Van Bo, Ward 12, District 4, Ho Chi Minh City

Contact person's name, position and contact details:

> Chuong Mai-Viet, Managing Director, chuong@fusetechnology.com.au

Activities relevant to the data transferred under these Clauses:

> Processing Support Data, Data Exporter's and their customer's personal data as reasonably necessary to maintain the relationship and provide contracted services to the Data Exporter and the Data Exporter's customers.

Signature and date: [*Chuong Mai-Viet* 2579A2BDA28A427…] on [17/1/2024].

16

Role (controller/processor):   Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

The personal data transferred concern the following categories of data subjects:

- Employees of the Data Exporter's group of companies,
- Contact details belonging to the Data Exporter's customers or prospective customers, and
- Distributer, re-seller, and partner contacts.

………………………..

Categories of personal data transferred

The personal data transferred concern the following categories of data:

- Employee information:
    - Name
    - Login details where applicable
    - Position
    - Department
    - Location
    - Contact number
    - Contact email address

    Rarely additional personal information may be transfered for a specific purpose, such as verification that criminal record and other identity checks have been completed.

    Bluesource Information Limited's Employee Privacy Policy provides more in depth information on personal information processed in relation to employees.

- Non employee contact information:

    - Name
    - Company
    - Department
    - Company Address
    - Contact numbers (landline, mobile, etc.)
    - Contact email address
    - Position

    Bluesource Information Limited's Privacy Policy provides more in depth information on personal information processed in relation to non-employees.

………………………..

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The personal data transferred concern the following special categories of data:

- Special categories of data are not procsessed other than date of birth, if reasonably required to be able to provide a service to the data subject, faciltate security requirements such as identity verification.
- The Data Exporter does not currently request or process the following special categories of personal information (as defined under GDPR):
    - Racial or Ethnic Origin (unless required to track equality in the workplace)
    - Political Opinions
    - Religious or philosophical beliefs
    - Trade Union Membership
    - Genetic Data
    - Biometric data
    - Data concerning sex life or sexual orientation

………………………..

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Personal data is held within the Data Exporter's systems which are hosted in the UK and/or EU geographies. The Data Importer accesses the data and/or enters relevant new/updated data as and when required to raise a support ticket for a Data Exporter's customer. Further processing by the Data Importer, for any other purpose, is not permitted.

…………………………

Nature of the processing

The personal data transferred will be subject to the following basic processing activities:

- Identity verification
- Facilitate logging in to systems and associated access control
- Information security
- Maintain the relationships between the Parties
- Process Support Data
- Processing for the purpose of being able to fulfil contractual and operational requirements, such as and not limited to logging and resolving support tickets and incidents for the Data Exporter's customers

Further processing by the Data Importer, for any other purpose, is not permitted.

…………………………

Purpose(s) of the data transfer and further processing

To fulful contractural obligations to the Data Exporter by providing adiitional resource as and when necessary, such as outside of the Data Exporter's business hours.

……………………..

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data is held within the Data Exporter's systems which are hosted in the UK and/or EU geographies. The Data Importer accesses the data and/or enters relevant new/updated data as and when required to raise a support ticket for a Data Exporter's customer. Further processing by the Data Importer, for any other purpose, is not permitted.

Access to the Data Exporter's system is controlled and managed by the Data Exporter, and the Data Importer only has access to the data as reasoably required for it to meet its contracted obligations.

…………………..

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The Data Importer is not permitted to use sub-processors, except where expressly permitted in writing by the Data Exporter.

…………………..

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The Information Commissioner's Office ("ICO").

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

It has been agreed between the Parties that the Data Importer, shall abide by bluesource's "DATA PROTECTION & INFORMATION SECURITY REQUIREMENTS FOR SUPPLIERS" policy which is available at: https://www.bluesource.co.uk/data-privacy-and-processing/, and as updated from time to time.

The Data Importer is not permitted to use sub-processors, except where expressly permitted in writing by the Data Exporter.

ANNEX III – LIST OF SUB-PROCESSORS

The Data Importer is not permitted to use sub-processors, except where expressly permitted in writing by the Data Exporter and recorded as a revsion under this Annex III.